OBLON, SPIVAK, ET AL
DOCKET #: 247305US6
INV: Ryo OCHI, et al.
SHEET 1 OF 14



FIG. 1

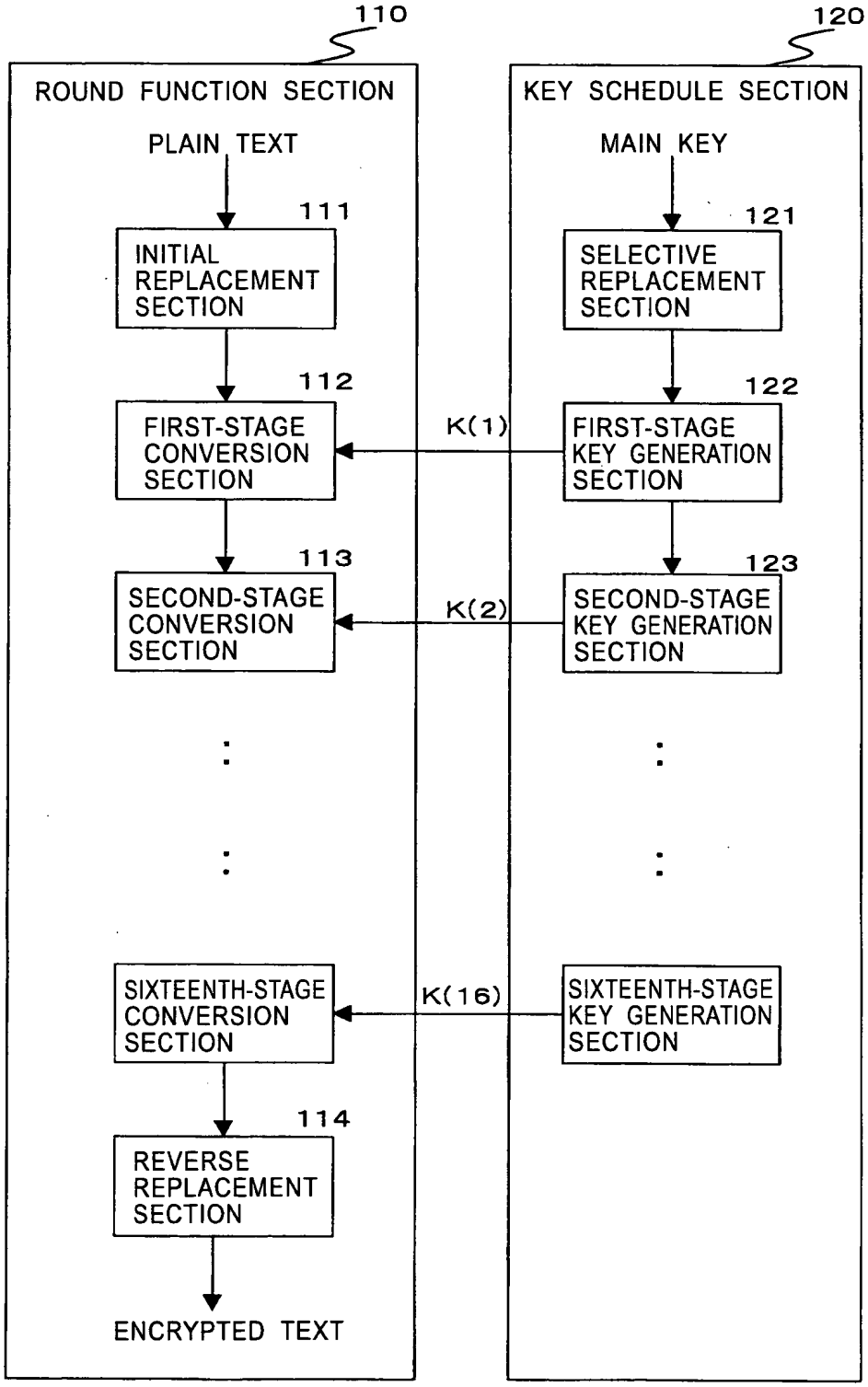


FIG. 2

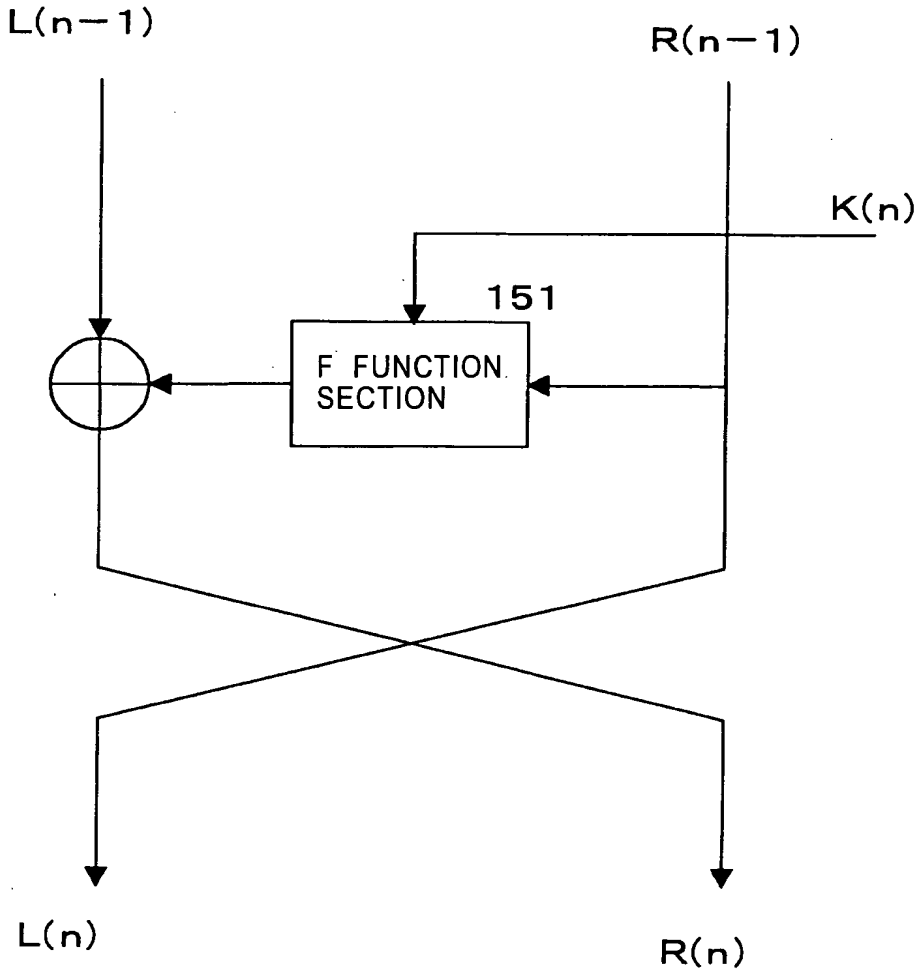


FIG. 3

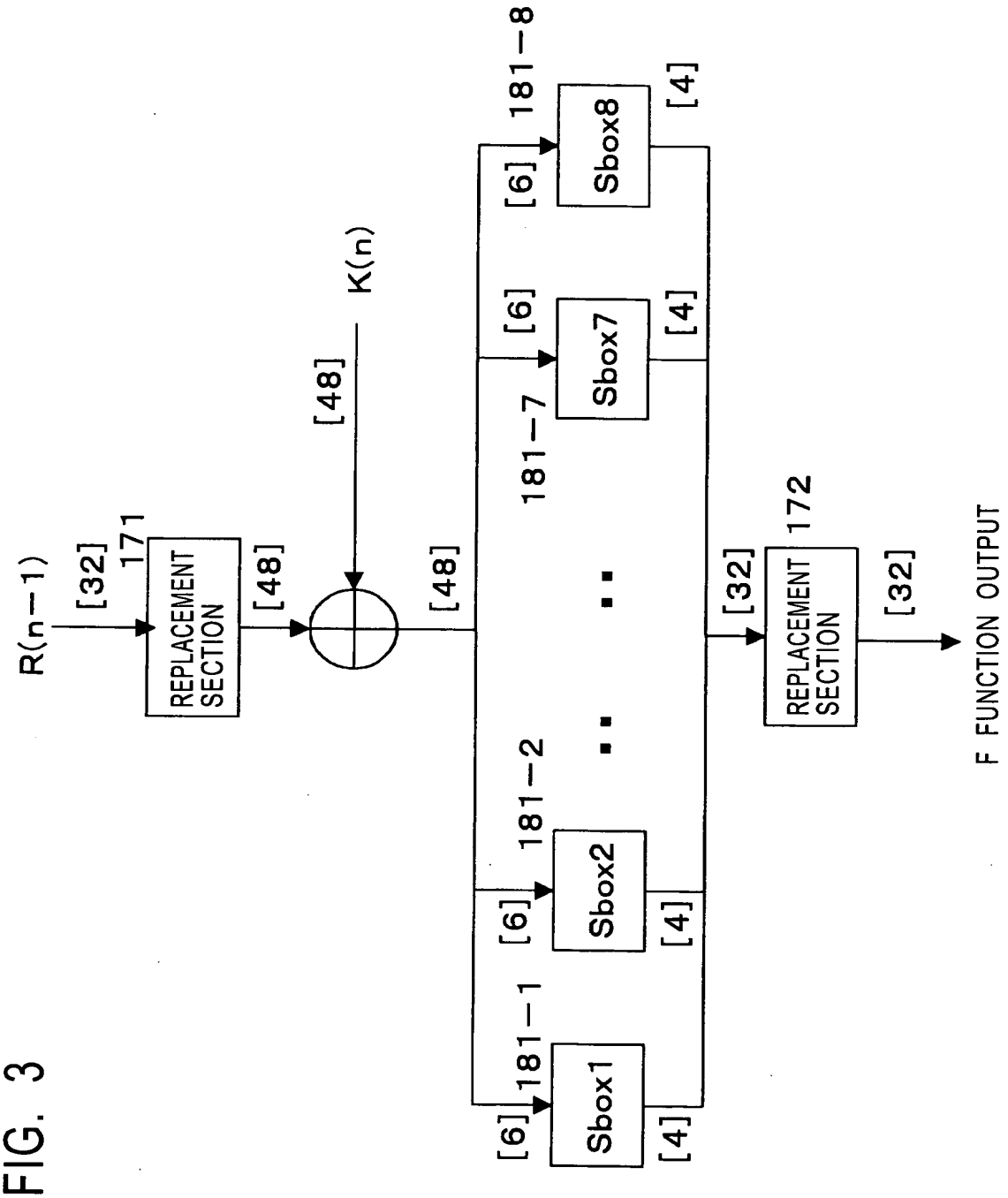

R(n−1)
[32]
171
REPLACEMENT SECTION
[48]
K(n)
[48]
[48]
[6]
181−8
Sbox8
[4]
[6]
Sbox7
[4]
181−7
[6]
181−2
Sbox2
[4]
[6]
181−1
Sbox1
[4]
[32]
172
REPLACEMENT SECTION
[32]
F FUNCTION OUTPUT

FIG. 4

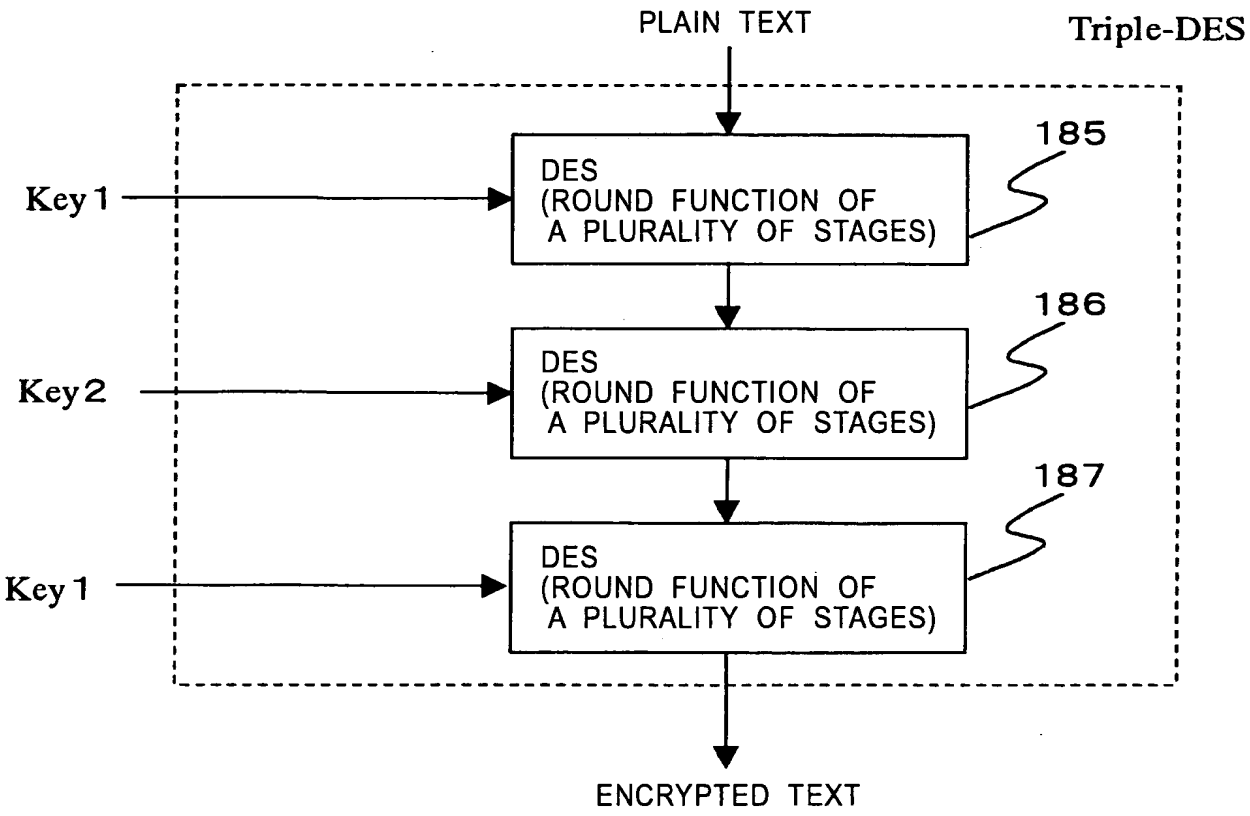

PLAIN TEXT
Triple-DES
185
DES
(ROUND FUNCTION OF
A PLURALITY OF STAGES)
Key 1
186
DES
(ROUND FUNCTION OF
A PLURALITY OF STAGES)
Key 2
187
DES
(ROUND FUNCTION OF
A PLURALITY OF STAGES)
Key 1
ENCRYPTED TEXT

FIG. 5

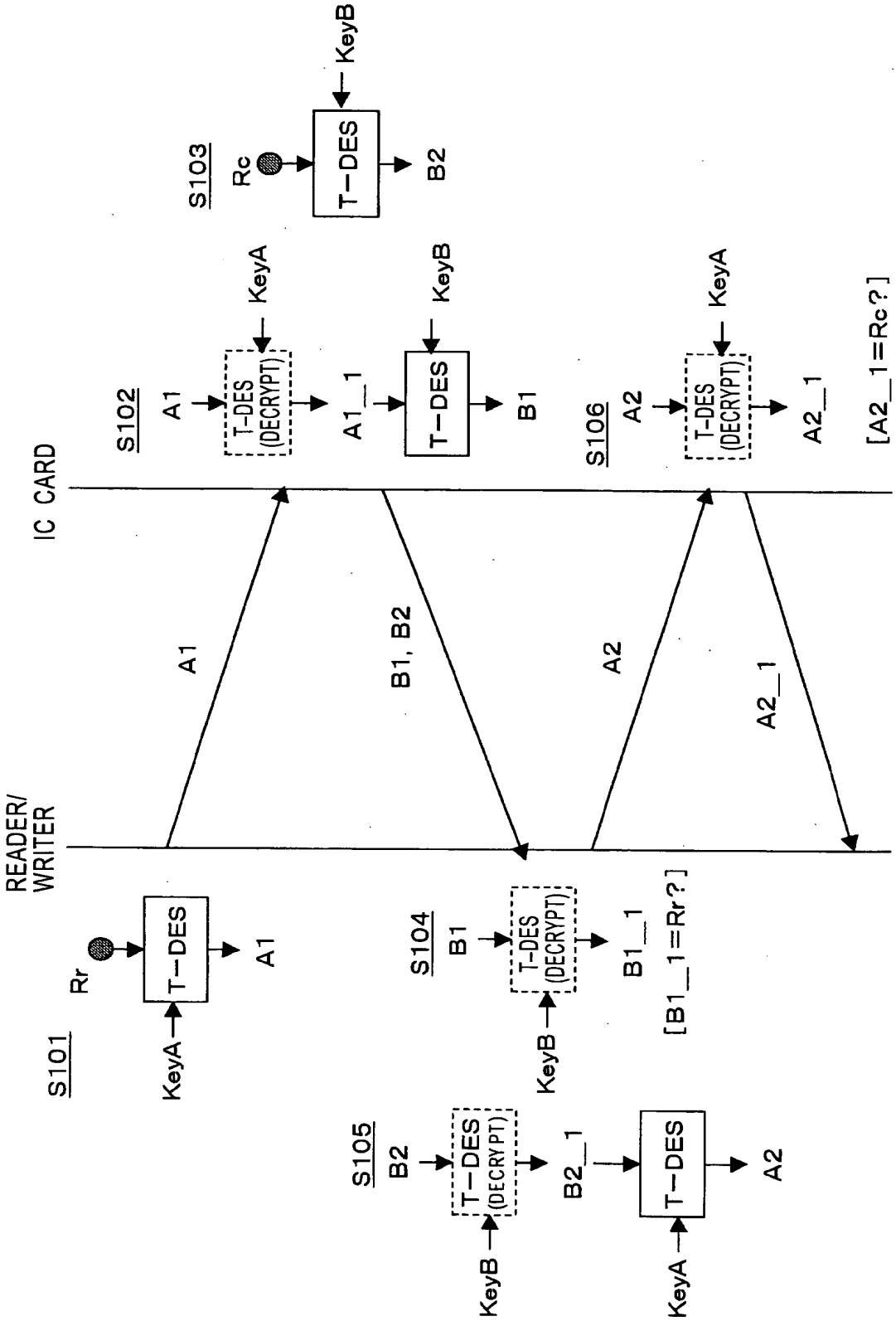

READER/
WRITER
IC CARD
S101
Rr
T-DES
KeyA
A1
S102
A1
T-DES
(DECRYPT)
KeyA
A1_1
T-DES
KeyB
B1
S103
Rc
T-DES
KeyB
B2
S104
B1
T-DES
(DECRYPT)
KeyB
B1_1
[B1_1=Rr?]
S105
B2
T-DES
(DECRYPT)
KeyB
B2_1
T-DES
KeyA
A2
S106
A2
T-DES
(DECRYPT)
KeyA
A2_1
[A2_1=Rc?]
A1
B1, B2
A2
A2_1

FIG. 6A

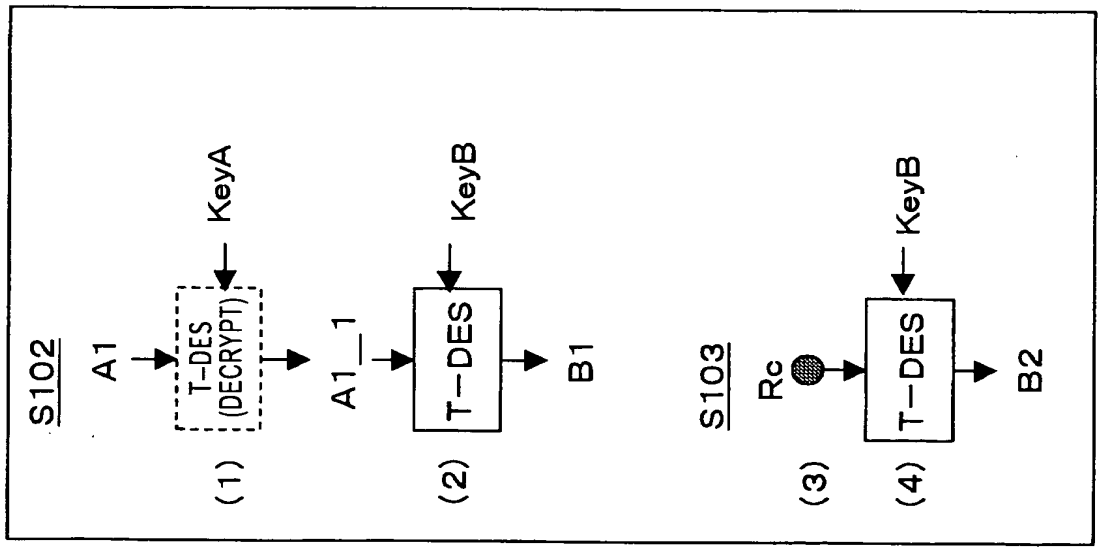

S102
A1
T-DES (DECRYPT)
KeyA
(1)
A1_1
T-DES
KeyB
(2)
B1
S103
Rc
(3)
T-DES
KeyB
(4)
B2

FIG. 6B

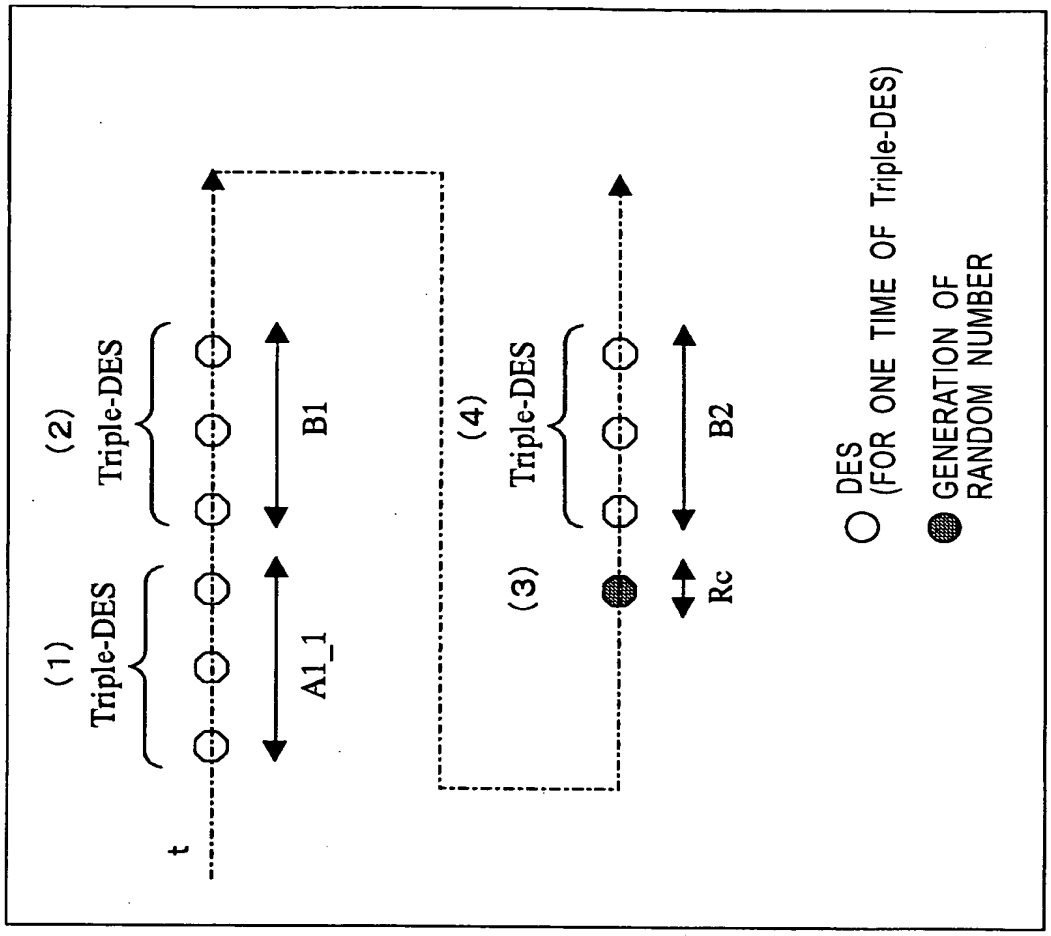

(1)
Triple-DES
(2)
Triple-DES
t
A1_1
B1
(3)
(4)
Triple-DES
Rc
B2
DES
(FOR ONE TIME OF Triple-DES)
GENERATION OF
RANDOM NUMBER

FIG. 7A

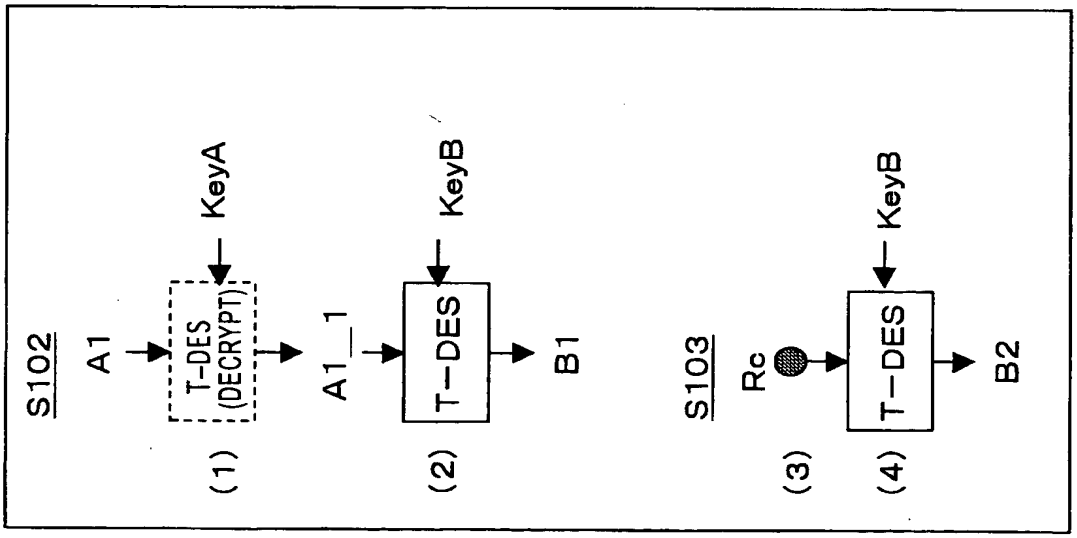

S102
A1
T-DES (DECRYPT)
KeyA
(1)
A1_1
T-DES
KeyB
(2)
B1
S103
Rc
(3)
T-DES
KeyB
(4)
B2

FIG. 7B

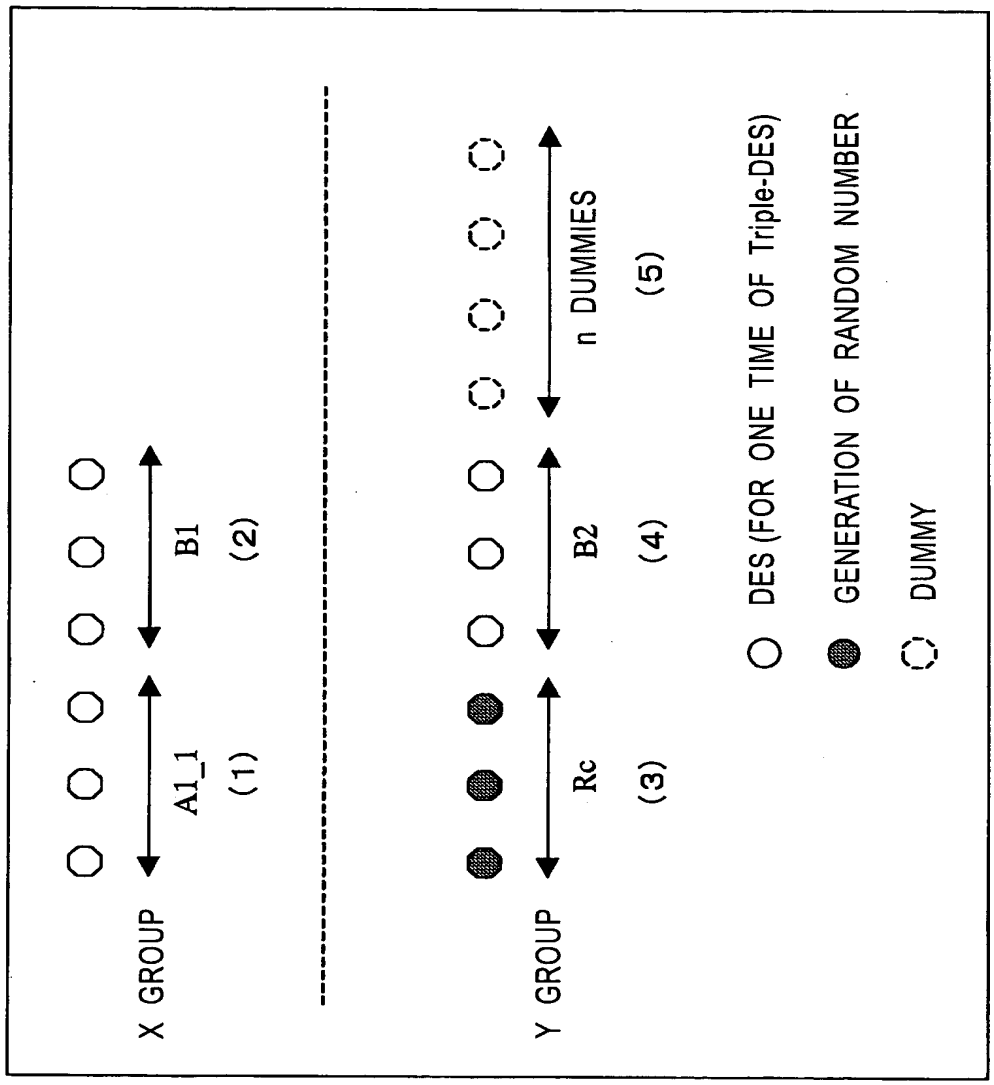

X GROUP
A1_1
(1)
B1
(2)
Y GROUP
Rc
(3)
B2
(4)
n DUMMIES
(5)
DES (FOR ONE TIME OF Triple-DES)
GENERATION OF RANDOM NUMBER
DUMMY

FIG. 8A

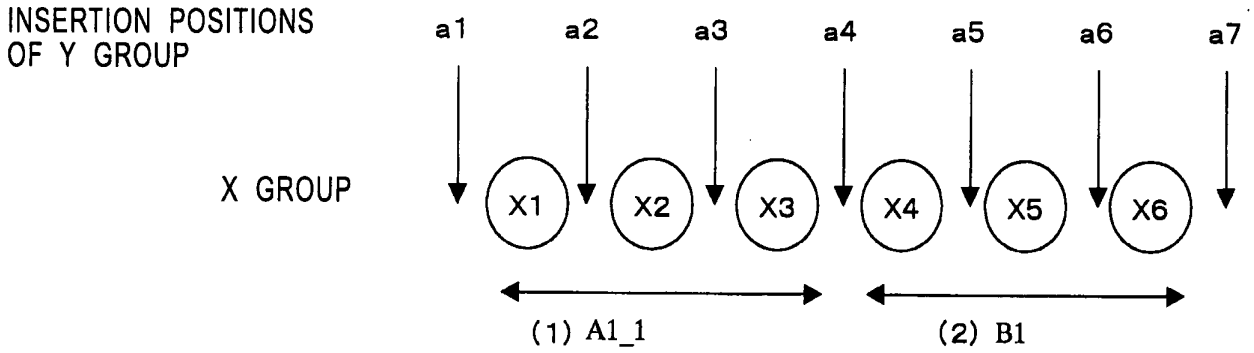



FIG. 8B

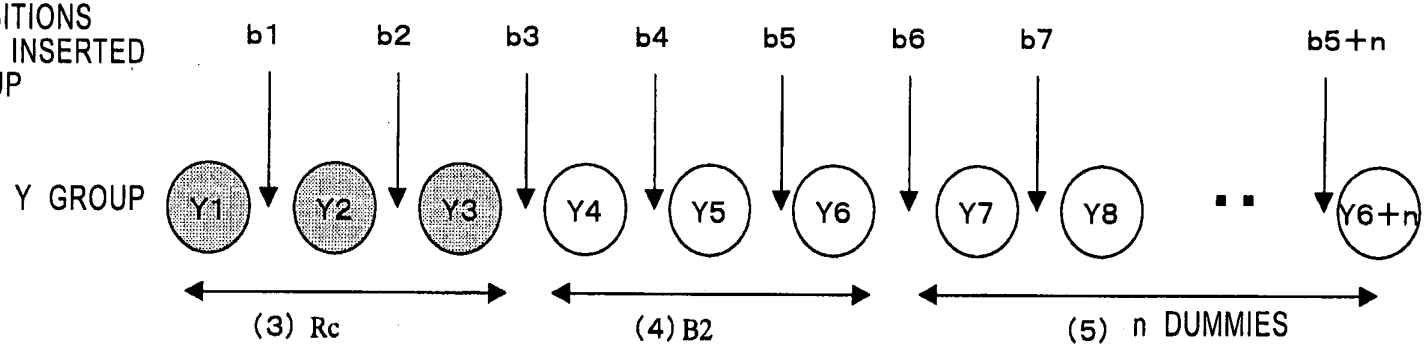



FIG. 8C

POSITIONS AT WHICH Y1 TO Y6, EXCLUDING DUMMIES, ARE ARRANGED IN 6+n OF Y GROUP

$$ {}_{6+n}C_{6} $$



OBLON, SPIVAK, ET AL
DOCKET #: 247305US6
INV: Ryo OCHI, et al.
SHEET 8 OF 14

FIG. 9

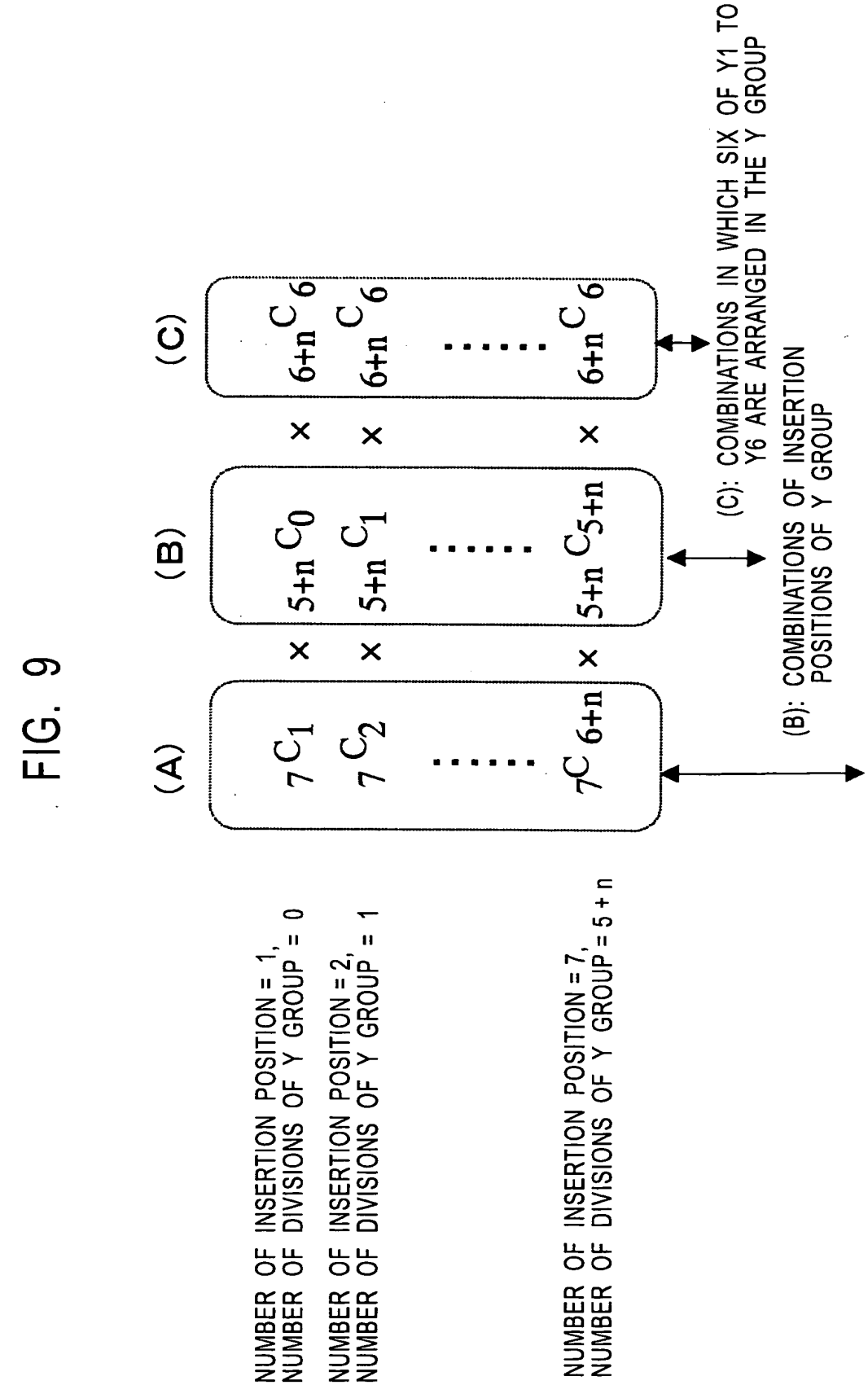
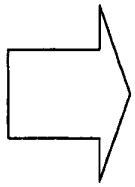

(A)
(B)
(C)
$_7C_1$ × $_{5+n}C_0$ × $_{6+n}C_6$
$_7C_2$ × $_{5+n}C_1$ × $_{6+n}C_6$
$_7C_{6+n}$ × $_{5+n}C_{5+n}$ × $_{6+n}C_6$
NUMBER OF INSERTION POSITION = 1,
NUMBER OF DIVISIONS OF Y GROUP = 0
NUMBER OF INSERTION POSITION = 2,
NUMBER OF DIVISIONS OF Y GROUP = 1
NUMBER OF INSERTION POSITION = 7,
NUMBER OF DIVISIONS OF Y GROUP = 5 + n
(C): COMBINATIONS IN WHICH SIX OF Y1 TO Y6 ARE ARRANGED IN THE Y GROUP
(B): COMBINATIONS OF INSERTION POSITIONS OF Y GROUP
(A): COMBINATIONS OF INSERTION POSITIONS OF Y GROUP IN THE X GROUP

FIG. 10A

NUMBER OF DUMMIES:
n = 0

$$
\begin{aligned}
{}_7C_1 \times {}_5C_0 \times 1 &= 7 \times 1 \times 1 = 7 \\
{}_7C_2 \times {}_5C_1 \times 1 &= 21 \times 5 \times 1 = 105 \\
{}_7C_3 \times {}_5C_2 \times 1 &= 35 \times 10 \times 1 = 350 \\
{}_7C_4 \times {}_5C_3 \times 1 &= 35 \times 10 \times 1 = 350 \\
{}_7C_5 \times {}_5C_4 \times 1 &= 21 \times 5 \times 1 = 105 \\
{}_7C_6 \times {}_5C_5 \times 1 &= 7 \times 1 \times 1 = 7
\end{aligned}
$$

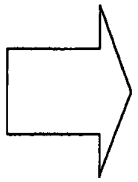


942 KINDS

FIG. 10B

NUMBER OF DUMMIES:
n = 3

$$
\begin{aligned}
{}_7C_1 \times {}_8C_0 \times {}_9C_6 &= 7 \times 1 \times 84 = 588 \\
{}_7C_2 \times {}_8C_1 \times {}_9C_6 &= 21 \times 8 \times 84 = 14112 \\
{}_7C_3 \times {}_8C_2 \times {}_9C_6 &= 35 \times 28 \times 84 = 82320 \\
{}_7C_4 \times {}_8C_3 \times {}_9C_6 &= 35 \times 56 \times 84 = 164640 \\
{}_7C_5 \times {}_8C_4 \times {}_9C_6 &= 21 \times 70 \times 84 = 123480 \\
{}_7C_6 \times {}_8C_5 \times {}_9C_6 &= 7 \times 56 \times 84 = 32928 \\
{}_7C_7 \times {}_8C_6 \times {}_9C_6 &= 1 \times 28 \times 84 = 2352
\end{aligned}
$$



420420 KINDS



OBLON, SPIVAK, ET AL
DOCKET #: 247305US6
INV: Ryo OCHI, et al.
SHEET 10 OF 14

FIG. 11

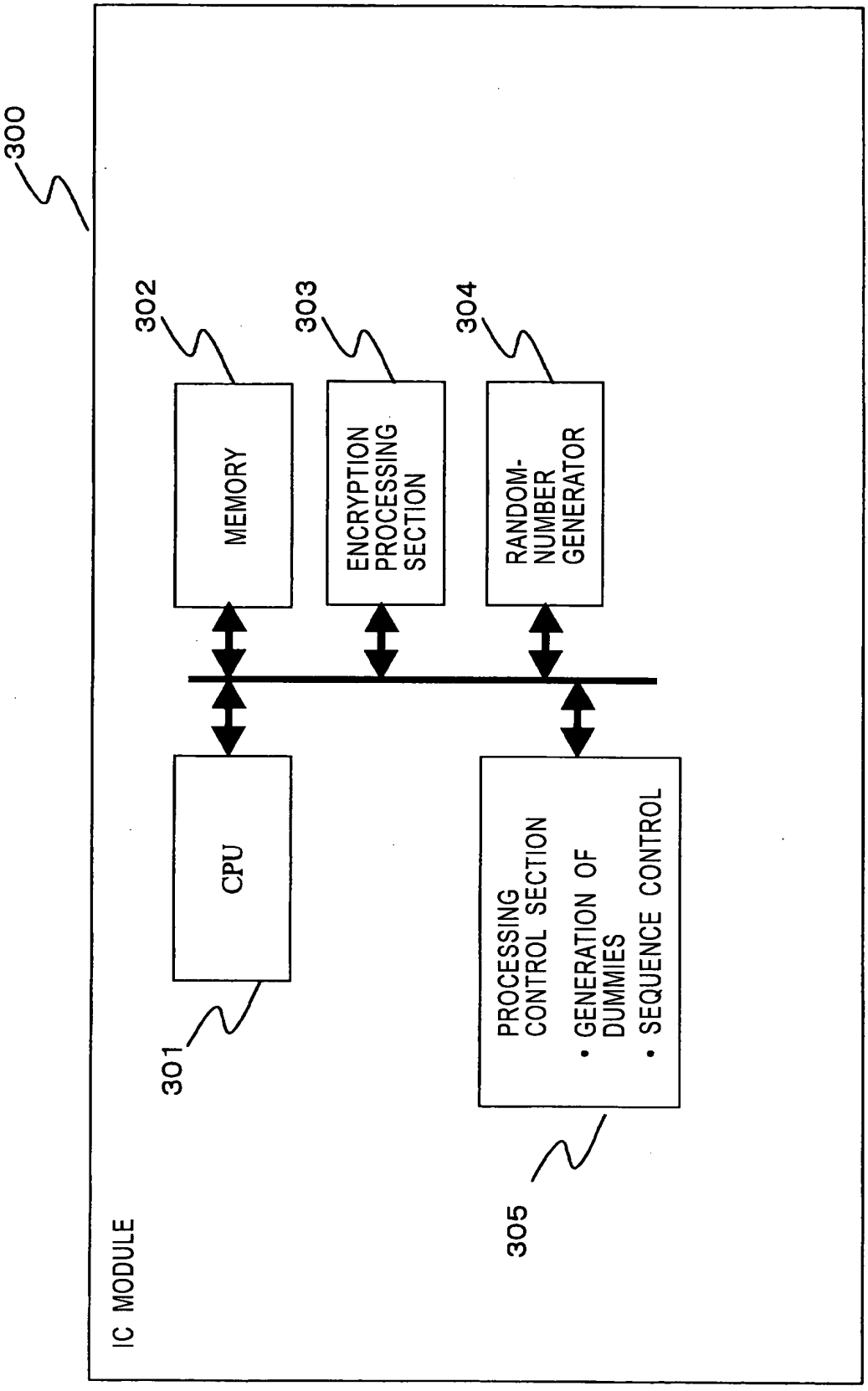

300
IC MODULE
302
MEMORY
303
ENCRYPTION PROCESSING SECTION
304
RANDOM-NUMBER GENERATOR
301
CPU
305
PROCESSING CONTROL SECTION
• GENERATION OF DUMMIES
• SEQUENCE CONTROL

FIG. 12

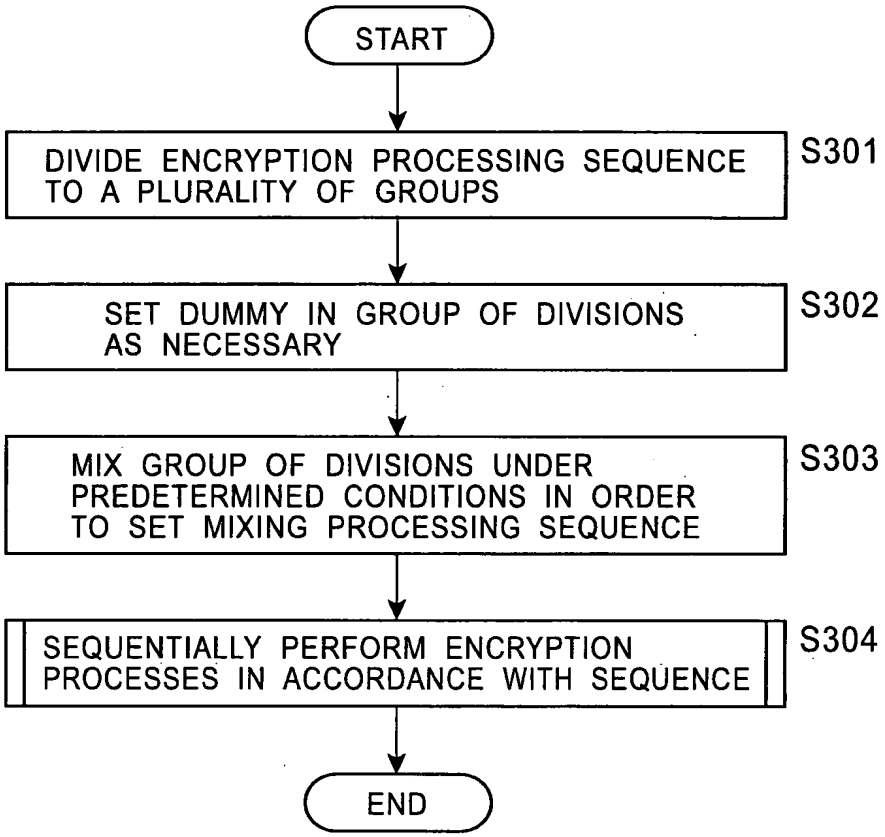

START
DIVIDE ENCRYPTION PROCESSING SEQUENCE TO A PLURALITY OF GROUPS
S301
SET DUMMY IN GROUP OF DIVISIONS AS NECESSARY
S302
MIX GROUP OF DIVISIONS UNDER PREDETERMINED CONDITIONS IN ORDER TO SET MIXING PROCESSING SEQUENCE
S303
SEQUENTIALLY PERFORM ENCRYPTION PROCESSES IN ACCORDANCE WITH SEQUENCE
S304
END

FIG. 13

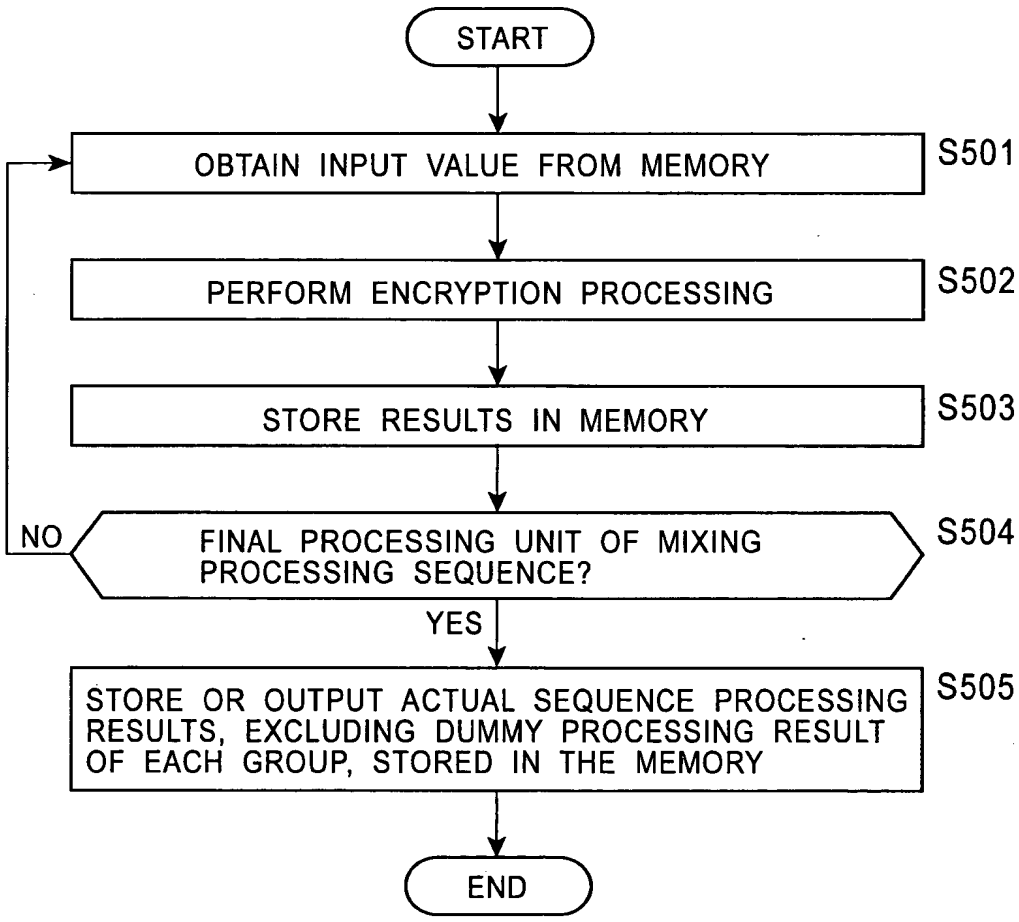
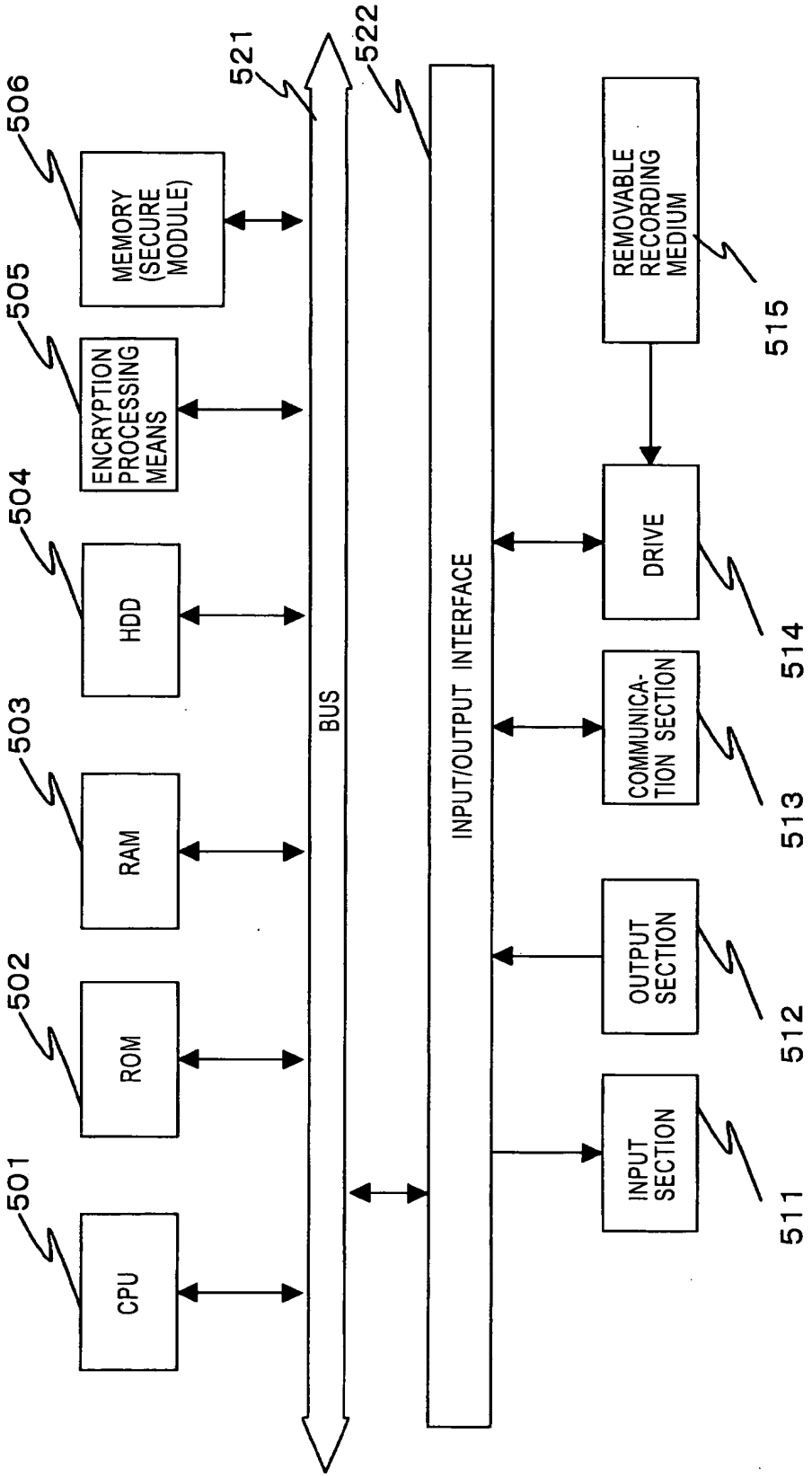

START
OBTAIN INPUT VALUE FROM MEMORY
S501
PERFORM ENCRYPTION PROCESSING
S502
STORE RESULTS IN MEMORY
S503
NO
FINAL PROCESSING UNIT OF MIXING PROCESSING SEQUENCE?
S504
YES
STORE OR OUTPUT ACTUAL SEQUENCE PROCESSING RESULTS, EXCLUDING DUMMY PROCESSING RESULT OF EACH GROUP, STORED IN THE MEMORY
S505
END

FIG. 14


521
522
506
MEMORY (SECURE MODULE)
505
ENCRYPTION PROCESSING MEANS
504
HDD
503
RAM
502
ROM
501
CPU
BUS
INPUT/OUTPUT INTERFACE
REMOVABLE RECORDING MEDIUM
515
DRIVE
514
COMMUNICATION SECTION
513
OUTPUT SECTION
512
INPUT SECTION
511